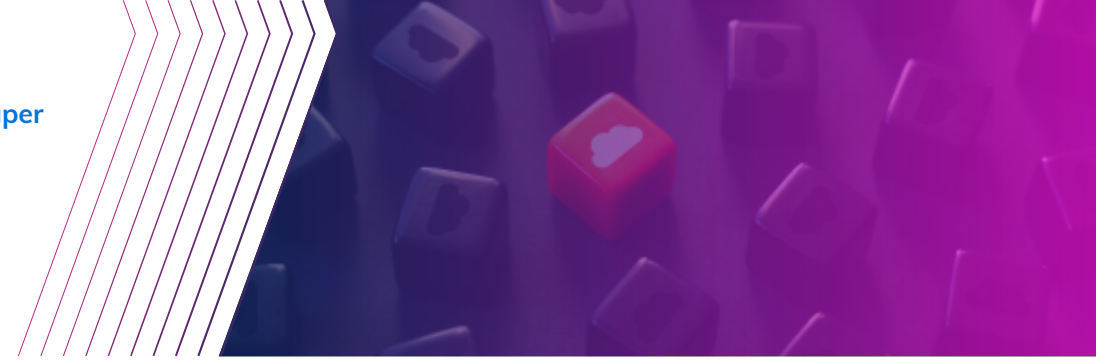
White paper

virtana

Security and Compliance



Introduction

The Virtana Platform delivers a comprehensive solution for IT Operations Management (ITOM), available both as a Software-as-a-Service (SaaS) offering and through a Kubernetes-based on-premises deployment model. The platform comprises key components such as Global View, Infrastructure Observability, and Container Observability. Central to Virtana's capabilities is its event intelligence and observability engine, which serves as a critical enabler for modern IT operations and DevOps methodologies. By providing real-time monitoring, sophisticated visualization, and advanced analytics, the platform equips organizations with deep visibility into the complexities of hybrid IT environments, encompassing applications, networks, and distributed systems. This whitepaper provides an in-depth examination of the security and compliance measures integrated within the Virtana Platform.

Overview

Virtana is dedicated to preserving the availability, integrity, and confidentiality of customer data which is of paramount importance in today's digital landscape. To achieve this, a multifaceted approach is essential. Virtana's multifaceted approach is focused on three key areas – data, product, and platform security.

Virtana is dedicated to preserving the **availability, integrity, and confidentiality** of customer data which is of paramount importance in today's digital landscape.

Data

Platform data security is an integral component of maintaining the trust and reliability of any technological ecosystem. Virtana encompasses a range of strategies and practices designed to safeguard sensitive information stored and processed within the platform.

At the core, the Virtana Platform only collects data needed for monitoring, management, and cost analysis of the managed environment; detailed data remains in the customer's environment. Virtana encrypts data both in transit and at rest, ensuring that the data remains indecipherable even if unauthorized access occurs.

Data Capture

Only IT elements managed by Virtana have data collected within a customer's environment. The type of data collected include:

- **Device and Conversation Metadata** – One of Virtana's strengths is its ability to discover infrastructure elements and understand their relationships through configuration data. This data is utilized to correlate events with specific elements, thereby narrowing the focus for Root Cause Analysis.
- **Performance data** – Virtana Infrastructure Observability captures system, storage, networking, and operating system performance data within the customer's environment. This data is then analyzed to provide the appropriate insights and actions.
- **Event data** – The Virtana Platform captures events from Virtana's tooling and 3rd-party systems to comprehend the health state of the managed environment.
- **Log data** – The Virtana Platform gathers log data from Loki.

Collection and Gateway Security

Virtana monitors and manages infrastructure across Hybrid IT environments through various methods, which could include probes, agents, or agentless collection. These methods are then consolidated at the virtual management appliance layer, which functions as a gateway/proxy. Through secure communication, this layer sends events to the Virtana Platform. Any requests for additional observability metrics made by Virtana's AI engine to resolve an event are directed to the gateway through that secure communication.

Deployment Architectures

Telemetry data for hosts, applications, storage devices, network switches, and Kubernetes clusters Is first gathered from our monitoring collector (installed on your cloud account or on-premises). This data is transmitted securely to the Virtana Event Collector API, which then gets processed and analyzed internally via our cloud services.

Integrations

Virtana Platform integrates with AWS, Azure, GCP, and our on-prem IO (Infrastructure Observability) or CO(Container Observability) tool. All integrations require basic authentication using user credentials. For IO, our Public API allows communication between external systems and the platform. External system interaction is restricted to HTTPS to allow for a secure communication channel.

The credentials provided require only read-only permissions to discover resources, their usage metrics, and costing metrics.

Telemetry data for hosts, applications, storage devices, network switches, and Kubernetes clusters Is first gathered from our monitoring collector (installed on your cloud account or on-premises).

Product

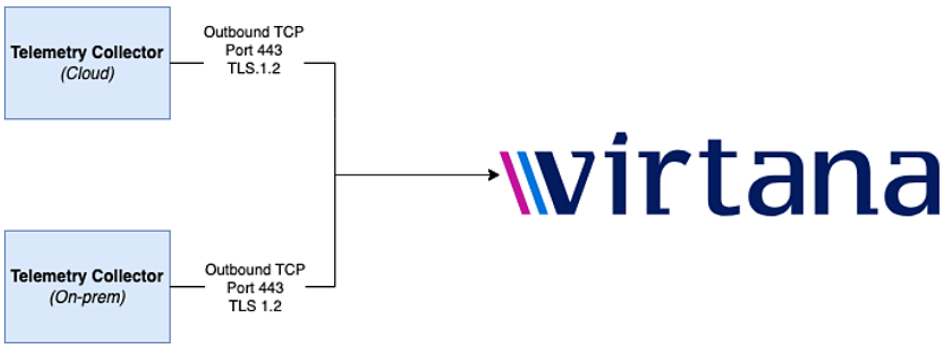
Product security is a fundamental aspect of the development lifecycle that focuses on ensuring the resilience and trustworthiness of software and hardware solutions. Virtana encompasses a series of measures and practices to identify, mitigate, and prevent a product's vulnerabilities and threats. This begins with secure design principles, where potential risks are considered from the outset and integrated security features are planned. Virtana performs rigorous testing, including vulnerability assessments and penetration testing, and provides regular security updates and patches to address newly discovered vulnerabilities, thereby maintaining the product's security posture over time.

AI and LLM

Virtana Copilot is powered by advanced AI, which enables it to understand and process natural language inputs effectively. Users interact with Copilot through a chat interface, typing questions or requests related to the Virtana Platform. Copilot then provides accurate and helpful information, drawing from Virtana's comprehensive documentation and real-time data. Copilot ensures that all interactions are handled securely. When you interact with the chatbot, your queries and any provided information are transmitted securely over encrypted channels. This ensures that your data is protected from unauthorized access during transmission. Virtana integrates with OpenAI for LLM support.

Audit Logs

We maintain logs of user activities. These logs include username, IP Address, date, and time of for all user actions. The data-access activity is logged within the access logs.



Communication Security

Virtana solutions use management appliances to gather real-time data pertinent to the health and performance of hybrid IT infrastructure. Communication from local or on-premises management appliance to the Virtana Platform is accomplished using a client identifier and secret, managed by the customer. These credentials are utilized to acquire a short-lived token, subsequently employed to securely publish data to the cloud and link it to the designated user organization. As these short- lived tokens expire, new tokens are automatically requested.

Data-in-motion:

- All data transmission is encrypted using TLS 1.2 with varying bit counts depending on the cipher used by the client.

Data-at-rest:

- For application monitoring, data at rest is encrypted using an AES-GCM-256-bit key for enhanced data protection.
- For cloud deployments, we use AWS Managed services for storing the data, and we follow AWS best practices to store the data. All the data stores are protected as per the AWS Well-Architected framework.
- For on-premises deployments, data-at-rest encryption depends on the customer's deployment model.

Identity Management

Identity management plays a crucial role in maintaining security and access control within digital environments. Organizations have two primary approaches to managing user identities effectively: built-in user management and external identity platforms.

- Built-in user management allows the use of your own system to create, authenticate, and authorize user identities.
- On-premises components behind firewalls can leverage LDAP to authenticate.
- External identity platforms, such as single sign-on (SSO) solutions by Okta, leverage third-party services to centralize identity management. Leveraging an SSO provider can also be configured for Multi-Factor Authentication.

The choice between these approaches depends on an organization's specific requirements, considering factors like scalability, integration capabilities, and the desired level of administrative control over user identities and access rights.

User Management

Within the Virtana Platform, administrators can provide user access using role-based access controls (RBAC). Customers can allocate roles to users according to their responsibilities. RBAC enables you to manage your users' access, viewing, and data management methods. In the context of container management, users can implement data separation at the cluster level.

Vulnerability Assessments

Early detection of security vulnerabilities is at the heart of our policies. We adhere to the NIST SSDF 1.1 framework by addressing security early in development through code reviews and approvals, Software Bill of Materials produced for every release, and ongoing security scanning.

Virtana products are scanned repeatedly on a scheduled basis against SAST, DAST, dependency and container scanning, infrastructure-as-code scanning, and secrets detection. Scans are run nightly and consolidated into a centralized vulnerability report. Security vulnerabilities are reviewed on a recurring basis, and exceptions discovered during code approvals are reviewed weekly.

Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their Severity. Upon becoming aware of such vulnerabilities, Virtana addresses critical and high vulnerabilities within 30 days, often sooner based on assessment, and medium vulnerabilities within 90 days.

Virtana engages to have independent penetration testing done annually by a third-party independent auditor. Virtana also runs regular vulnerability scans for the Cloud Environment using updated vulnerability databases.

Platform

Virtana Platform leverages multiple layers of defense to provide a secure cloud platform to our customers. Our architecture, cloud operations, access and authentication, and deployment architecture are designed with security and protection considerations.

Platform Availability

Virtana Platform is built for 99.5 % availability. Refer here for more details. The platform is designed for high availability with multiple Availability Zones. For container management and IPM use cases, users can enable disaster recovery.

The status of the Virtana Platform can be tracked at https://status.cloud.virtana.com.

Platform Architecture

The Virtana Platform environment is hosted on AWS across two different geographies to cater to our global customers. For geographies where Virtana is not currently available, the platform can be quickly extended into other regions if a suitable business need emerges. Data replication across geographies does not occur due to sovereignty and data protection regulations.

Geography	Locations
North America	US Central
Europe	United Kingdom

Platform Compliance

Virtana ensures compliance with recognized industry standards related to data security and privacy, thus ensuring that sensitive data remains protected and operational services remain resilient over an extended period.

- **SOC 2 Type 2:** Virtana's company infrastructure, software, people, data, policies, procedures, and operations have been formally reviewed and are SOC 2 Type 2 compliant. SOC2 Type 2 detailed report can be obtained through your account executive.